Como garantir a segurança da informação

Carsten Rudolph e Roland Rieke, da Fraunhofer SIT (Alemanha)

A Internet do futuro compreenderá canais de comunicação físicos subjacentes, sob o controle de várias operadoras e redes sobrepostas, como infraestruturas P2P de baixo nível, redes industriais de controle, redes privadas virtuais, jogos, infraestruturas de serviços, computação em nuvem e backbones lógicos. Como garantir a segurança das informações nesse novo ambiente? Veja a resposta a seguir.

As atuais infraestruturas de informação e comunicação (a Internet, em sentido amplo) consistem de vários protocolos, diferentes tecnologias subjacentes para conectar dispositivos e transmitir dados e diferentes camadas de aplicações distribuídas. Algumas das tecnologias e protocolos são transparentes do ponto de vista do usuário. Essa tendência continuará até que o transporte de dados seja realmente perfeito, de forma que os usuários e também as aplicações não mais tenham conhecimento da tecnologia usada. Assim, a Internet do futuro de fato consistirá de canais de comunicação físicos subjacentes, sob o controle de várias operadoras e redes sobrepostas, como infraestruturas P2P de baixo nível, redes industriais de controle, redes privadas virtuais, redes de jogos, infraestruturas de serviços, infraestruturas de computação em *cloud* (nuvem) e backbones lógicos.

No nível dos usuários e das aplicações, apenas algumas dessas redes sobrepostas são relevantes e visíveis. Os usuários envolvidos podem ser indivíduos, mas também empresas ou governos. Obviamente, um importante efeito é que as fronteiras entre as infraestruturas tecnológicas de comunicação estão ocultas. Uma tendência nova e também crescente é um desenvolvimento similar em níveis mais altos. Há uma interseção de várias redes sobrepostas e os usuários nem sempre estão cientes que suas atividades na Internet podem se relacionar com várias redes sobrepostas. Portanto, as fronteiras também desaparecem no nível lógico de aplicações e serviços. Um exemplo é o uso de um *login* para uma rede lógica particular (por exemplo, uma rede social) como algum tipo mecanismo de assinatura para serviços em outras redes lógicas.

Do ponto de vista de confiabilidade e de segurança, a Internet do futuro terá de fornecer mecanismos de segurança que não diminuam o potencial de uso da infraestrutura como um todo. A identificação e a autorização precisam ser fáceis e flexíveis. Soluções federadas, assinatura única ou mecanismos avançados como identificação baseada em RFID – identificação por radiofrequência, serão usadas para diferentes graus de identificação pessoal. Ao mesmo tempo, a Internet será ainda mais inescrutável. Torna-se cada vez mais difícil para os usuários comuns e até para usuários profissionais (empresas) compreender e apreender as consequências de suas ações na Internet. A distribuição de dados privados ocorrerá através das fronteiras hoje visíveis.

O artigo a seguir se baseia nos projetos europeus Massif, SecFutur e AsserT4SOA.

Visão

Uma Internet totalmente segura continuará sendo uma ilusão (similar a todas as sociedades humanas). Entretanto, no mundo "físico", as pessoas têm a percepção dos riscos a que se expõem. Numa cidade, pode-se saber que áreas são seguras e quais devem ser evitadas. Além disso, nas redes sociais físicas há o estabelecimento de relações de confiança (quase sempre

dependentes do comportamento) e consegue-se a identificação por vários meios não técnicos. Não se pode transferir isso tudo para a Internet com facilidade.

Ao contrário das infraestruturas de TI existentes, a Internet do futuro deverá fornecer suporte inerente para a confiabilidade e a segurança, em termos das chamadas áreas de confiança. Essa área de confiança não deve se restringir a uma rede física particular ou a uma rede sobreposta de aplicação. Uma área de confiança deve cruzar várias camadas e se posicionar ortogonalmente em relação às diferentes redes sobrepostas. Dentro de uma área de confiança, os usuários devem poder estabelecer relações de confiança e saber e ser informados do que podem fazer com segurança e quais são os riscos. A consequência não é que haja sempre um alto nível de segurança dentro de uma área de confiança, mas que se possa ter uma boa garantia do comportamento resultante e das propriedades da segurança.

Pode-se comparar uma área de confiança a uma comunidade social (ou a uma cidade), onde os cidadãos sabem em quem confiar e em que áreas podem morar, fazer compras, comer fora com segurança, e em que áreas devem ter maior cuidado. A Internet do futuro suportará uma infraestrutura de confiança com suporte inerente a áreas de confiança, como meios confiáveis para fornecer o conhecimento de segurança situacional para os usuários.

Prevemos que esse tipo de conhecimento situacional já possa ser fornecido pela próxima geração de ambientes de SIEM - informações de segurança e gerenciamento de eventos. A implantação do SIEM tradicional ocorre dentro de uma infraestrutura corporativa. Quando é um provedor externo que fornece um serviço SIEM, em geral, também é o caso em que a sua implantação está dentro da esfera da organização do provedor e que os eventos somente passam via cliente interno ou enlaces do provedor de serviços.

Entretanto, um cenário de implantação futura é possibilidade de os enlaces entre dispositivos gerenciados e a organização do provedor de serviço serem vias públicas da Internet. Esse último caso é onde a evolução da Internet, com sua inerente falta de segurança holística, é relevante para SIEM e a Internet como canal torna-se um motivo de preocupação. É possível usar áreas de confiança para aumentar os sistemas SIEM com seus próprios mecanismos de segurança. Além disso, o SIEM na Internet também poderia ser implantado como serviços do tipo *cloud*.

Desafios

Áreas de confiança são uma nova forma de olhar as relações de confiança e a segurança na Internet. Requerem uma combinação dos mecanismos de segurança existentes e, dependendo das propriedades de segurança a serem atendidas dentro uma área de confiança, pode ser necessário combinar a segurança baseada em hardware com autorização de usuário, tecnologias de preservação de privacidade e mecanismos de contabilização seguros.

A implantação de um SIEM em um modo do tipo *cloud* demandaria outra forma de pensar o modelo de obtenção de receita, assim como a forma os clientes seriam cobrados por serviços 'sob demanda'. O número de eventos sozinho não é necessariamente um bom indicador, mas o número de sistemas poderia ser aceitável. Uma taxa baseada no número de incidentes detectados seria atraente para um provedor, mas poderia levar a controvérsias entre cliente e provedor com relação ao que é declarado como incidente.

Em essência, no entanto, a Internet está promovendo um completo repensar do paradigma segundo o qual as organizações implantam e gerenciam suas próprias infraestruturas para muitos aspectos de suas necessidades computacionais.

A Internet em evolução, portanto, traz algumas novas questões para a implantação de SIEM e, do ponto de vista do SIEM, reforça a importância de ter uma Internet com segurança e serviços possivelmente diferenciados para controle de tráfego de 'alta prioridade', como os eventos de um SIEM. Os modelos comerciais também mudam, uma vez que a 'taxa de serviço' precisa evoluir para poder escalar para cima ou para baixo.

Os modelos *pay-per-use* (pagar o consumido) são possíveis e as organizações podem evitar investimentos (Capex) e pagamentos recorrentes de custos (Opex).

O desenvolvimento das áreas de confiança da Internet do futuro e da próxima geração de SIEM requer os seguintes pontos:

• identificar as necessidades de confiança e segurança das diferentes partes interessadas;
• identificar os mecanismos de segurança disponíveis e integrá-los em protocolos, dispositivos, interfaces, políticas, etc.;
• integrar áreas de confiança às aplicações para que os usuários fiquem cientes das relações de confiança ou automaticamente decidir quanto à satisfação de políticas;
• desenvolver meios confiáveis e resilientes para fornecer aos usuários consciência da segurança situacional; e
• estabelecer tipos avançados de gerenciamento de segurança distribuída para áreas de confiança, incluindo os meios para uma configuração de evolução adaptativa de medidas de segurança, de acordo com a evolução da infraestrutura e das redes sobrepostas e o conhecimento situacional sobre as atuais ameaças e atividades espúrias.

Outros desafios resultam da importância da Internet do futuro para as sociedades modernas. Partes essenciais da sociedade dependerão da Internet do futuro. São exemplos a distribuição de energia, a comunicação corporativa ou o transporte e o tráfego.

Soluções

Muitos desafios e tópicos de pesquisa permanecem em aberto para o estabelecimento das áreas de confiança da Internet do futuro. Algumas das soluções possíveis são:

• Identificação e atestado de estado e configuração do dispositivo para o estabelecimento e manutenção de relações de confiança em um nível técnico.
• Estabelecimento de backbones confiáveis de Internet do futuro como raiz de confiança para a comunicação.
• Informação de segurança e gerenciamento de evento (SIEM) distribuído, hierárquico, celular.
• Distribuição restrita de dados dentro de uma área de confiança particular no nível de aplicação ou mesmo num nível de pacotes.
• Interfaces de serviços cientes da segurança e certificação de segurança de nível de serviço.
• Informação de segurança e gerenciamento de evento (SIEM) avançado: resiliência (segurança automática, tolerância à intrusão, autoproteção e autocura); descentralização (hierárquica ou celular; distribuição de aquisição e processamento, perfeita divisão de funções entre equipamentos de núcleo e coletores de borda); e abertura (comunicação de backbone baseada em Internet resiliente, processamento baseado em computação nas nuvens seguro e confiável).